Intelligence Reform and Terrorism Prevention Act of 2004, Sec 1016, Information Sharing

Core-Awareness-Training

PDF [1]

SEC. 1016. INFORMATION SHARING.

(a) DEFINITIONS.--In this section:

(1) HOMELAND SECURITY INFORMATION.?The term ?homeland security information? has the meaning given that term in section 892(f) of the Homeland Security Act of 2002 (6 U.S.C. 482(f))

(2) INFORMATION SHARING COUNCIL.--The term ``Information Sharing Council'' means the Information Systems Council established by Executive Order 13356, or any successor body designated by the President, and referred to under subsection (g).

(3) INFORMATION SHARING ENVIRONMENT; ISE.--The terms ``information sharing environment'' and ``ISE'' mean an approach that facilitates the sharing of terrorism and homeland security information, which approach may include any methods determined necessary and appropriate for carrying out this section.

(4) PROGRAM MANAGER.--The term ``program manager'' means the program manager designated under subsection (f).

(5) TERRORISM INFORMATION.--The term ``terrorism information'' --

(A) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to--

> (i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
>
> (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
>
> (iii) communications of or by such groups or individuals; or
>
> (iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and

(B) includes weapons of mass destruction information.

(6) WEAPONS OF MASS DESTRUCTION INFORMATION.?The term ?weapons of mass destruction information? means information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or a terrorist organization against the United States,

including information about the location of any stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or a terrorist organization against the United States.

(b) INFORMATION SHARING ENVIRONMENT.--

(1) ESTABLISHMENT.--The President shall--

(A) create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties;

(B) designate the organizational and management structures that will be used to operate and manage the ISE; and

(C) determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.

(2) ATTRIBUTES.--The President shall, through the structures described in subparagraphs (B) and (C) of paragraph (1), ensure that the ISE provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. The President shall, to the greatest extent practicable, ensure that the ISE provides the functional equivalent of, or otherwise supports, a decentralized, distributed, and coordinated environment that--

(A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;

(B) ensures direct and continuous online electronic access to information;

(C) facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations and operations;

(D) builds upon existing systems capabilities currently in use across the Government;

(E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;

(F) facilitates the sharing of information at and across all levels of security;

(G) provides directory services, or the functional equivalent, for locating people and information;

(H) incorporates protections for individuals' privacy and civil liberties;

(I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls;

(J) integrates the information within the scope of the information sharing environment, including any such information in legacy technologies;

(K) integrates technologies, including all legacy technologies, through Internet-based services, consistent with appropriate security protocols and safeguards, to enable connectivity among required users at the Federal, State, and local levels;

(L) allows the full range of analytic and operational activities without the need to centralize information within the scope of the information sharing environment;

(M) permits analysts to collaborate both independently and in a group (commonly known as ?collective and noncollective collaboration?), and across multiple levels of national security information and controlled unclassified information;

(N) provides a resolution process that enables changes by authorized officials regarding rules and policies for the access, use, and retention of information within the scope of the information sharing environment; and

(O) incorporates continuous, real-time, and immutable audit capabilities, to the maximum extent practicable

(c) PRELIMINARY REPORT.--Not later than 180 days after the date of the enactment of this Act, the program manager shall, in consultation with the Information Sharing Council--

(1) submit to the President and Congress a description of the technological, legal, and policy issues presented by the creation of the ISE, and the way in which these issues will be addressed;

(2) establish an initial capability to provide electronic directory services, or the functional equivalent, to assist in locating in the Federal Government intelligence and terrorism information and people with relevant knowledge about intelligence and terrorism information; and

(3) conduct a review of relevant current Federal agency capabilities, databases, and systems for sharing information.

(d) GUIDELINES AND REQUIREMENTS.--As soon as possible, but in no event later than 270 days after the date of the enactment of this Act, the President shall--

(1) leverage all ongoing efforts consistent with establishing the ISE and issue guidelines for acquiring, accessing, sharing, and using information, including guidelines to ensure that information is provided in its most shareable form, such as by using tearlines to separate out data from the sources and methods by which the data are obtained;

(2) in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061, issue guidelines that--

(A) protect privacy and civil liberties in the development and use of the ISE; and

(B) shall be made public, unless nondisclosure is clearly necessary to protect national security; and

(3) require the heads of Federal departments and agencies to promote a culture of information sharing by--

(A) reducing disincentives to information sharing, including over-classification of information and unnecessary requirements for originator approval, consistent with applicable laws and regulations; and

(B) providing affirmative incentives for information sharing.

(e) IMPLEMENTATION PLAN REPORT.--Not later than one year after the date of the enactment of this Act, the President shall, with the assistance of the program manager, submit to Congress a report containing an implementation plan for the ISE. The report shall include the following:

(1) A description of the functions, capabilities, resources, and conceptual design of the ISE, including standards.

(2) A description of the impact on enterprise architectures of participating agencies.

(3) A budget estimate that identifies the incremental costs associated with designing, testing, integrating, deploying, and operating the ISE.

(4) A project plan for designing, testing, integrating, deploying, and operating the ISE.

(5) The policies and directives referred to in subsection (b)(1)(C), as well as the metrics and enforcement mechanisms that will be utilized.

(6) Objective, systemwide performance measures to enable the assessment of progress toward achieving the full implementation of the ISE.

(7) A description of the training requirements needed to ensure that the ISE will be adequately implemented and properly utilized.

(8) A description of the means by which privacy and civil liberties will be protected in the design and operation of the ISE.

(9) The recommendations of the program manager, in consultation with the Information Sharing Council, regarding whether, and under what conditions, the ISE should be expanded to include other intelligence information.

(10) A delineation of the roles of the Federal departments and agencies that will participate in the ISE, including an identification of the agencies that will deliver the infrastructure needed to operate and manage the ISE (as distinct from individual department or agency components that are part of the ISE), with such delineation of roles to be consistent with--

(A) the authority of the Director of National Intelligence under this title, and the amendments made by this title, to set standards for information sharing throughout the intelligence community; and

(B) the authority of the Secretary of Homeland Security and the Attorney General, and the role of the Department of Homeland Security and the Attorney General, in coordinating with State, local, and tribal officials and the private sector.

(11) The recommendations of the program manager, in consultation with the Information Sharing Council, for a future management structure for the ISE, including whether the position of program manager should continue to remain in existence.

(f) PROGRAM MANAGER.--

(1) DESIGNATION.--Not later than 120 days after the date of the enactment of this Act, with notification to Congress, the President shall designate an individual as the program manager responsible for information sharing across the Federal Government. The individual designated as the program manager shall serve as program manager until removed from service or replaced by the President (at the President's sole discretion). The program manager, in consultation with the head of any affected department or agency, shall have and exercise governmentwide authority over the sharing of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, by all Federal departments,

agencies, and components, irrespective of the Federal department, agency, or component in which the program manager may be administratively located, except as otherwise expressly provided by law.

(2) DUTIES AND RESPONSIBILITIES.--

(A) IN GENERAL.--The program manager shall, in consultation with the Information Sharing Council--

(i) plan for and oversee the implementation of, and manage, the ISE;

(ii) assist in the development of policies, as appropriate, to foster the development and proper operation of the ISE;

(iii) consistent with the direction and policies issued by the President, the Director of National Intelligence, and the Director of the Office of Management and Budget, issue governmentwide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE;

(iv) identify and resolve information sharing disputes between Federal departments, agencies, and components; and

(v) assist, monitor, and assess the implementation of the ISE by Federal departments and agencies to ensure adequate progress, technological consistency and policy compliance; and regularly report the findings to Congress.

(B) CONTENT OF POLICIES, PROCEDURES, GUIDELINES, RULES, AND STANDARDS.--The policies, procedures, guidelines, rules, and standards under subparagraph (A)(ii) shall--

(i) take into account the varying missions and security requirements of agencies participating in the ISE;

(ii) address development, implementation, and oversight of technical standards and requirements;

(iii) take into account ongoing and planned efforts that support development, implementation and management of the ISE;

(iv) address and facilitate information sharing between and among departments and agencies of the intelligence community, the Department of Defense, the homeland security community and the law enforcement community;

(v) address and facilitate information sharing between Federal departments and agencies and State, tribal, and local governments;

(vi) address and facilitate, as appropriate, information sharing between Federal departments and agencies and the private sector;

(vii) address and facilitate, as appropriate, information sharing between Federal departments and agencies with foreign partners and allies; and

(viii) ensure the protection of privacy and civil liberties.

(g) INFORMATION SHARING COUNCIL.--

(1) ESTABLISHMENT.--There is established an Information Sharing Council that shall assist the

President and the program manager in their duties under this section. The Information Sharing Council shall serve until removed from service or replaced by the President (at the sole discretion of the President) with a successor body.

(2) SPECIFIC DUTIES.--In assisting the President and the program manager in their duties under this section, the Information Sharing Council shall--

(A) advise the President and the program manager in developing policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE;

(B) work to ensure coordination among the Federal departments and agencies participating in the ISE in the establishment, implementation, and maintenance of the ISE;

(C) identify and, as appropriate, recommend the consolidation and elimination of current programs, systems, and processes used by Federal departments and agencies to share information, and recommend, as appropriate, the redirection of existing resources to support the ISE;

(D) identify gaps, if any, between existing technologies, programs and systems used by Federal departments and agencies to share information and the parameters of the proposed information sharing environment;

(E) recommend solutions to address any gaps identified under subparagraph (D);

(F) recommend means by which the ISE can be extended to allow interchange of information between Federal departments and agencies and appropriate authorities of State and local governments;

(G) assist the program manager in identifying and resolving information sharing disputes between Federal departments, agencies, and components;

(H) identify appropriate personnel for assignment to the program manager to support staffing needs identified by the program manager; and

(I) recommend whether or not, and by which means, the ISE should be expanded so as to allow future expansion encompassing other relevant categories of information.

(3) CONSULTATION.--In performing its duties, the Information Sharing Council shall consider input from persons and entities outside the Federal Government having significant experience and expertise in policy, technical matters, and operational matters relating to the ISE.

(4) INAPPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.--The Information Sharing Council (including any subsidiary group of the Information Sharing Council) shall not be subject to the requirements of the Federal Advisory Committee Act (5 U.S.C. App.).

(5) DETAILEES.?Upon a request by the Director of National Intelligence, the departments and agencies represented on the Information Sharing Council shall detail to the program manager, on a reimbursable basis, appropriate personnel identified under paragraph (2)(H).;

(h) PERFORMANCE MANAGEMENT REPORTS.--

(1) IN GENERAL.--Not later than two years after the date of the enactment of this Act, and not later than June 30 of each year thereafter, the President shall submit to Congress a report on the state of the ISE and of information sharing across the Federal Government.

(2) CONTENT.--Each report under this subsection shall include--

(A) a progress report on the extent to which the ISE has been implemented, including how the ISE has fared on the performance measures and whether the performance goals set in the preceding year have been met;

(B) objective system-wide performance goals for the following year;

(C) an accounting of how much was spent on the ISE in the preceding year;

(D) actions taken to ensure that procurement of and investments in systems and technology are consistent with the implementation plan for the ISE;

(E) the extent to which all terrorism watch lists are available for combined searching in real time through the ISE and whether there are consistent standards for placing individuals on, and removing individuals from, the watch lists, including the availability of processes for correcting errors;

(F) the extent to which State, tribal, and local officials are participating in the ISE;

(G) the extent to which private sector data, including information from owners and operators of critical infrastructure, is incorporated in the ISE, and the extent to which individuals and entities outside the government are receiving information through the ISE;

(H) the measures taken by the Federal government to ensure the accuracy of information in the ISE, in particular the accuracy of information about individuals;

(I) an assessment of the privacy and civil liberties protections of the ISE, including actions taken in the preceding year to implement or enforce privacy and civil liberties protections; and

(J) an assessment of the security protections used in the ISE.

(i) AGENCY RESPONSIBILITIES.--The head of each department or agency that possesses or uses intelligence or terrorism information, operates a system in the ISE, or otherwise participates (or expects to participate) in the ISE shall-

(1) ensure full department or agency compliance with information sharing policies, procedures, guidelines, rules, and standards established under subsections (b) and (f);

(2) ensure the provision of adequate resources for systems and activities supporting operation of and participation in the ISE;

(3) ensure full department or agency cooperation in the development of the ISE to implement governmentwide information sharing; and

(4) submit, at the request of the President or the program manager, any reports on the implementation of the requirements of the ISE within such department or agency.

(j) Report on the Information Sharing Environment.?

(1) IN GENERAL.?Not later than 180 days after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, the President shall report to the Committee on Homeland Security and Governmental Affairs of the Senate, the Select Committee on Intelligence of the Senate, the Committee on Homeland Security of the House of Representatives, and the Permanent

Select Committee on Intelligence of the House of Representatives on the feasibility of?

(A) eliminating the use of any marking or process (including ?Originator Control?) intended to, or having the effect of, restricting the sharing of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, between and among participants in the information sharing environment, unless the President has?

(i) specifically exempted categories of information from such elimination; and

(ii) reported that exemption to the committees of Congress described in the matter preceding this subparagraph; and

(B) continuing to use Federal agency standards in effect on such date of enactment for the collection, sharing, and access to information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, relating to citizens and lawful permanent residents;

(C) replacing the standards described in subparagraph (B) with a standard that would allow mission-based or threat-based permission to access or share information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, for a particular purpose that the Federal Government, through an appropriate process established in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061, has determined to be lawfully permissible for a particular agency, component, or employee (commonly known as an ?authorized use? standard); and

(D) the use of anonymized data by Federal departments, agencies, or components collecting, possessing, disseminating, or handling information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, in any cases in which?

(i) the use of such information is reasonably expected to produce results materially equivalent to the use of information that is transferred or stored in a non-anonymized form; and

(ii) such use is consistent with any mission of that department, agency, or component (including any mission under a Federal statute or directive of the President) that involves the storage, retention, sharing, or exchange of personally identifiable information

(2) DEFINITION.?In this subsection, the term ?anonymized data? means data in which the individual to whom the data pertains is not identifiable with reasonable efforts, including information that has been encrypted or hidden through the use of other technology.

(k) Additional Positions.?The program manager is authorized to hire not more than 40 full-time employees to assist the program manager in?

(1) activities associated with the implementation of the information sharing environment, including?

(A) implementing the requirements under subsection (b)(2); and

(B) any additional implementation initiatives to enhance and expedite the creation of the information sharing environment; and

(2) identifying and resolving information sharing disputes between Federal departments, agencies, and components under subsection (f)(2)(A)(iv).

(l) Authorization of Appropriations.?There is authorized to be appropriated to carry out this section $30,000,000 for each of fiscal years 2008 and 2009

Links:
[1] http://www.ise.gov/sites/default/files/IRTPA_amended.pdf